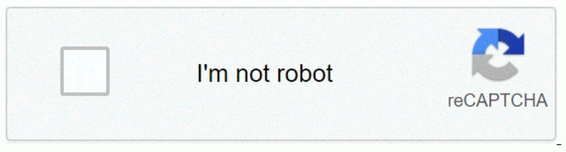
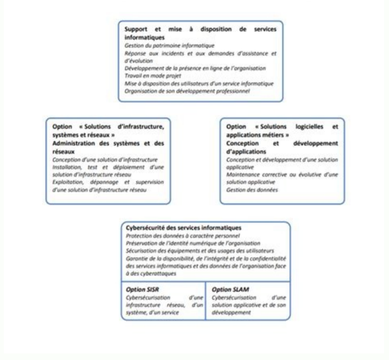



I'm not robot!

# Cours bts sio sisr pdf

accueilaccueil.txt · Dernière modification: 2023/05/25 10:23 de techer.charles_educ-valadon-limoges.fr Titre Public Matières Présentation Type Date de Modification Mots Clés Utilisation de la distribution Kali dans le cadre du bloc 3 sur la cybersécurité v2 + MITM BTS SIO Bloc 3 - Cybersécurité des services informatiques, Bloc 3 - Cybersécurité des services informatiques - SISR Activités en laboratoire permettant d'exploiter la distribution Kali Linux dans le cadre du bloc 3 sur la cybersécurité. Deux laboratoires composés de machines virtuelles sur VirtualBox sont fournis (connexion requise) ↓ ↓ .... LABORATOIRE 07/11/2022 Kali, cryptographie, chiffrement, certificat, analyse trames, empoisonnement arp, scanner de vulnérabilités, exploitation de vulnérabilités, exploit, metasploit, payloads, hameçonnage, typosquattage, typosquating, ingénierie sociale, dns spoofing, remédiations, hygiène numérique, respect des bonnes pratiques. Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques BTS SIO Bloc 3 - Cybersécurité des services informatiques - SISR Activités en laboratoire du bloc 3 Cybersécurité spécialité SISR concernant la mise en place d'un équipement de gestion unifiée des menaces informatiques dans un contexte plus large. Cet ensemble d'activités lié au bloc 3 Cybersécurité... LABORATOIRE 14/07/2022 Bonnes pratiques, protocoles DNS, HTTP, HTTPS, LDAP, VPN IPsec, VPN SSL, routage, NAT, filtrage, IPS/IDS, portail captif, proxy web. Attaque MITM d'un service SSH et mise en place de contre-mesures BTS SIO Bloc 3 - Cybersécurité des services informatiques - SISR Après avoir remobilisé les savoirs fondamentaux en matière de cryptographie, ce TP permet de mettre en évidence certaines vulnérabilités du service SSH. À travers l'exploitation de ces vulnérabilités, l'étudiant sera amené à approfondir le... LABORATOIRE 03/09/2021 cryptographie, chiffrement, exploitation de vulnérabilités, remédiations, hygiène numérique, respect des bonnes pratiques de sécurité. Utilisation de la distribution Kali dans le cadre du bloc 3 sur la cybersécurité v1 - Contexte Box to Bed BTS SIO Bloc 3 - Cybersécurité des services informatiques, Bloc 3 - Cybersécurité des services informatiques - SISR, Bloc 3 - Cybersécurité des services informatiques - SLAM Fiches pratiques de travaux en laboratoire permettant d'exploiter la distribution Kali Linux dans le cadre du bloc 3 sur la cybersécurité. Une fiche est commune aux deux options puis chaque option dispose de deux fiches spécifiques. LABORATOIRE 28/05/2021 Kali, metasploit, wireshark, chiffrement, scanner de vulnérabilités.
Scénario pédagogique pour le Bloc 3 SISR du BTS SIO BTS SIO Bloc 3 - Cybersécurité des services informatiques - SISR Principes didactiques retenus pour le scénario Le référentiel du BTS SIO est désormais organisé en blocs de compétences afin de suivre les préconisations de la loi n° 2014-288 du 5 mars 2014 sur la formation professionnelle... DIDACTIQUE 17/05/2021 Scénarios pédagogiques du CNED pour le BTS SIO 2020 BTS SIO Bloc 1 - Support et mise à disposition de services informatiques, Bloc 3 - Cybersécurité des services informatiques, Bloc 2 - Administration des systèmes et des réseaux, Bloc 3 - Cybersécurité des services informatiques - SISR, Bloc 2 - Conception et développement d'applications, Bloc 3 - Cybersécurité des services informatiques - SLAM Le CNED a commandé la rédaction de nouveaux cours pour le BTS SIO rénové. A cette fin, des scénarios pédagogiques ont été conçus pour ces étudiants qui travaillent à distance. Avec l'accord du CNED, ces scénarios sont publiés ici pour la communauté des... DIDACTIQUE 20/08/2020 Scénarios pédagogiques Sécurité informatique et cybercriminalité Terminale STMG, BTS SIO, Autres BTS tertiaires Management, sciences de gestion et numérique, Enseignement spécifique de systèmes d'information de gestion, Bloc 3 - Cybersécurité des services informatiques, Bloc 3 - Cybersécurité des services informatiques - SISR, Bloc 3 - Cybersécurité des services informatiques - SLAM Cette ressource permet aux élèves/étudiants, placés dans le contexte d'une organisation, de découvrir les divers aspects de la sécurité et les moyens de protection face aux menaces informatiques, en groupe de TP (salle informatique). COURS 30/06/2020 Sécurité informatique, cybercriminalité, cybersécurité, RGPD, CNIL, BlockChain Côté labo : Installation et sécurisation de Nextcloud BTS SIO Bloc 2 - Administration des systèmes et des réseaux, Bloc 3 - Cybersécurité des services informatiques - SISR L'objectif global est de découvrir Nextcloud puis de mettre l'accent sur un aspect lié à sa sécurisation, à savoir la prévention des attaques par dictionnaire. Les objectifs intermédiaires sont donc : d'avoir une vue d'ensemble de... LABORATOIRE 15/03/2019 Nextcloud, Fail2ban, attaque par dictionnaire, Python, Mechanize, sécurité. Téléphonie IP avec Asterisk (GSB) BTS SIO Bloc 2 - Administration des systèmes et des réseaux, Bloc 3 - Cybersécurité des services informatiques - SISR Ce Côté Labo a pour objectif de mettre en place une maquette complète de ToIP autour du serveur IPBX Asterisk. Au delà de la présentation des fonctionnalités de base offertes par le logiciel, les travaux menés permettent d'illustrer un aspect lié à la... LABORATOIRE 16/12/2016 ToIP, VoIP, Asterisk, MITM, ARP Poisonning, chiffrement TLS, softphone Exolab : Activité Packet Tracer de découverte - Access-lists (règles de filtrage) CISCO BTS SIO Bloc 2 - Administration des systèmes et des réseaux, Bloc 3 - Cybersécurité des services informatiques - SISR, SISR2 Conception des infrastructures réseaux Cette activité propose plusieurs scénarios de filtrage, permettant de comprendre le fonctionnement des access-lists CISCO, appliquées aux interfaces de routeur, en entrée et en sortie. Les 7 scénarios proposés permettent d'aborder successivement... EXOLAB 23/03/2016 Packet Tracer, Activité, Maquette, Filtrage, Pare-Feu, Access-List, ACL. sisr1:route_td1 Vos devez compléter le réseau simulé avec Packet Tracer (réseau partiel du BTS SIO et du contexte M2L) afin que les ordinateurs de M2L puissent communiquer avec Internet. Voici l'évolution du schéma à réaliser : La liaison entre le routeur Rectorat et le routeur du FAI est une liaison distante entre deux routeurs est représentée avec un éclair rouge dans le logiciel Packet Tracer. Dans cet exemple, La liaison entre le routeur R1 et le routeur R2 est de type série DCE avec une fréquence d'horloge de 64 000. Résultat à obtenir : tous les ordinateurs doivent pouvoir accéder au serveur Web avec son nom DNS www.m2m.local. Voici le fichier Packet tracer de départ qu'il faudra modifier pour ajouter la liaison distante : reseaubtssio_m2l_vlan.pkt Configuration des deux Routeur Rectorat et FAI : ajoutez sur chaque routeur un module de liaison série WIC-2T créer une liaison série entre ces deux routeurs configurez les interfaces du Routeur du Rectorat vers Routeur FAI : 196.5.0.1/24 configurez les interfaces du Routeur du FAI vers Routeur Rectorat : 196.5.0.2/24 vers Serveur Web&DNS : 194.2.0.1/24 Schéma Packet tracer avec liaison distante : reseaubtssio_m2l_vlan_serie.pkt Les ordinateurs du réseau M2L ne peuvent communiquer avec ceux du BTSSIO. Il est nécessaire d'ajouter une route sur le routeur du Rectorat à cet effet : Router>enable Router#conf t Router(config)#ip route 172.16.0.0 255.255.0.0 10.187.37.252 Router(config)#end Router#write Pour supprimer une route : Router(config)#no ip route 172.16.0.0 255.255.0.0 10.187.37.252 Router(config)#ip route 0.0.0.0 0.0.0.0 196.5.0.2 Ajoutez toutes les routes statiques nécessaires pour que la communication soit possible entre les ordinateurs des sous-réseau et avec le serveur Web&DNS. Ressource : La connexion au routeur s'effectue par le port console en utilisant la ligne associée à ce port ou bien à distance en utilisant les lignes virtuelles (appelées VTY). Ces ports virtuels sont utilisés pour les connexions telnet ou ssh. Par défaut, il n'y a pas de compte créé pour l'authentification. Si un mot de passe n'est pas configuré les accès distants ne sont pas autorisés. Donc au départ, seul l'accès à la console est autorisé.




Il faut créer au minimum un mot de passe pour l'accès aux différents terminaux (console et virtuel) et un mot de passe pour l'accès au mode privilégié (enable). Le mode d'administration par défaut est telnet. Par défaut, les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration.

Il faut tout d'abord activer le service encryption-password pour que les mots de passe apparaissent chiffrés lorsque les commandes d'affichage de la configuration sont entrées.
Router(config)#service password-encryption Router(config)#do show line Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int * 0 CTY - - - - - 0 0 0/0 - 65 AUX 9600/9600 - - - - - 0 0 0/0 - 66 VTY - - - - - 0 0 0/0 - 67 VTY - - - - - 0 0 0/0 - 68 VTY - - - - - 0 0 0/0 - 69 VTY - - - - - 0 0 0/0 - 70 VTY - - - - - 0 0 0/0 - Line(s) not in async mode -or- with no hardware support: 1-64 Router(config)# Il y a un port console (CTY), un port auxiliaire (AUX) et cinq ports pour les accès distants (VTY). Un mot de passe doit être créé pour se loguer aux différentes lignes. Router(config)#enable secret motdepasseenable Router(config)#line con 0 Router(config-line)#password motdepasseconsole Router(config-line)#login Router(config-line)#exit Router(config)#line vty 0 4 Router(config-line)#password motdepassevty Router(config-line)#login Router(config-line)#end Router# Il y a maintenant un mot de passe à saisir pour l'accès distant (telnet par défaut) au routeur et un mot de passe à saisir pour l'accès au mode avec privilège. En mode console il faudra alors : saisir le mot de passe console (motdepasseconsole) saisir le mot de passe enable pour avoir un accès au mode privilège (motdepasseenable) User Access Verification Password: motdepasseconsole Router>enable Password: motdepasseenable Router# sisr1/route_td1.txt · Dernière modification: 2018/01/23 23:56 (modification externe)